White Paper – March 2021

# ALL ABOUT AUTHENTICATION:
# A Health-ISAC Guide for CISOs

H-ISAC™
HEALTH - ISAC

www.h-isac.org

## SCOPE STATEMENT

# MANAGING AUTHENTICATION

**MFA. OTP. FIDO. SMS. PKI. All of these acronyms might have you saying OMG, but they are each important to understand when it comes to managing authentication.**

It's an anomaly these days when a major breach happens and compromised authentication systems don't play a role. Multi Factor Authentication (MFA) is critical to stopping attacks — but as we'll detail in this paper, not all MFA is the same, and attackers are catching up to some first-generation MFA tools. Health CISOs need to stay ahead of the curve.

This is the third installment in the H-ISAC's ongoing series focused on helping CISOs implement an identity-centric approach to cybersecurity. Our first paper, *Identity for the CISO Not Yet Paying Attention to Identity*, explained why identity matters. We followed that with *An H-ISAC Framework for CISOs to Manage Identity*, outlining how CISOs can implement a comprehensive approach to identity-centric security that will protect against modern attacks and support key business drivers.

Now we're going to start diving deeper into different areas of that framework, starting with authentication. Most cybersecurity professionals know that authentication is important, but many do not understand the differences between various authentication tools or how to best implement it in their organization. This paper was written to address those questions and includes two case studies detailing how different health organizations have implemented strong authentication.

## KEY TAKEAWAYS

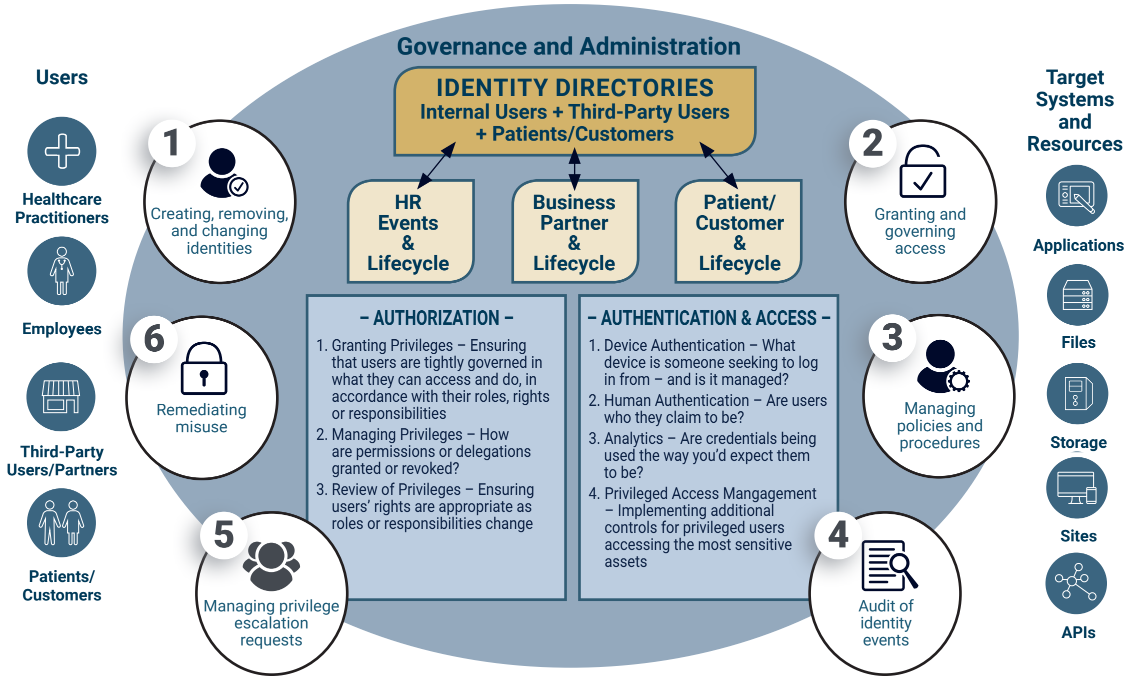
1. Passwords alone offer minimal security; MFA is essential.
2. Not all MFA is the same. Attackers have found ways to phish authentication technologies such as one-time passwords (OTPs) that are based on "shared secrets." Wherever possible, use high assurance, phishing-resistant tools such as FIDO or Public Key Infrastructure (PKI).
3. Usability matters. MFA implementations struggle if they degrade the user experience. Modern MFA solutions offer streamlined authentication processes that are easier to use than passwords.
4. Where feasible, move from static MFA to a multi-layered approach that integrates signals from device authentication and analytics tools to enable continuous, risk-based authentication.

# INTRODUCTION

The playbook for attackers is almost a cliché: First, a compromised password is used to establish access to a system. And second, attackers exploit inadequate Identity and Access Management (IAM) controls to access data that should be restricted — often in combination with escalation of privilege — allowing them to exfiltrate sensitive data. Authentication is the initial attack point; blocking these attacks lets you stop most breaches.[1]

As our previous papers outlined, authentication is not the only thing that matters. The *H-ISAC Framework for CISOs to Manage Identity* details how different Identity and Access Management (IAM) tools can be integrated via a holistic framework that enables an enterprise to manage the full identity lifecycle of employees, practitioners, patients, and business partners in a way that guards against common attacks on identity, materially lowers risk, and increases operational efficiencies.

**An H-ISAC Framework for Managing Identity**


Governance and Administration
Users
Healthcare Practitioners
Employees
Third-Party Users/Partners
Patients/ Customers
IDENTITY DIRECTORIES
Internal Users + Third-Party Users + Patients/Customers
HR Events & Lifecycle
Business Partner & Lifecycle
Patient/ Customer & Lifecycle
1 Creating, removing, and changing identities
2 Granting and governing access
3 Managing policies and procedures
4 Audit of identity events
5 Managing privilege escalation requests
6 Remediating misuse
Target Systems and Resources
Applications
Files
Storage
Sites
APIs

– AUTHORIZATION –

1. Granting Privileges – Ensuring that users are tightly governed in what they can access and do, in accordance with their roles, rights or responsibilities
2. Managing Privileges – How are permissions or delegations granted or revoked?
3. Review of Privileges – Ensuring users' rights are appropriate as roles or responsibilities change

– AUTHENTICATION & ACCESS –

1. Device Authentication – What device is someone seeking to log in from – and is it managed?
2. Human Authentication – Are users who they claim to be?
3. Analytics – Are credentials being used the way you'd expect them to be?
4. Privileged Access Mangagement – Implementing additional controls for privileged users accessing the most sensitive assets

With regard to authentication, the paper included two key points:

- Organizations should use MFA, given how easy it has become for hackers to compromise a password. Years of breaches means that more than 15 billion compromised credentials are now available in hacker forums.[2] Between password reuse, password spraying, and phishing attacks, passwords no longer offer meaningful security.
- Ideally, organizations should go a step beyond static MFA to embrace a multi-layered approach that enables continuous, risk-based authentication.

[1] Note that in the 2020 SolarWinds incident, attackers bypassed some MFA; however, it was the use of MFA that ultimately led to the attack being discovered. FireEye got an alert that someone had tried to register a new device to the company's MFA system that was not recognized, generating an alert. See https://news.yahoo.com/hackers-last-year-conducted-a-dry-run-of-solar-winds-breach-215232815.html

[2] https://www.bleepingcomputer.com/news/security/over-15-billion-credentials-in-circulation-on-hacker-forums/

## AUTHENTICATION BASICS

For years, NIST and other security experts have classified authentication into three categories:

- **Something you know –** like a password, PIN, or the answer to a "security question" (i.e., what high school did you attend?)
- **Something you have –** like a security key, smart ID card, one-time password (OTP) token, or smartphone
- **Something you are –** most commonly, biometrics such as fingerprint or face

The formula for MFA has traditionally been pretty simple: Augment a password with an authentication factor from one of the other two categories.

However, not all of these categories are equal in strength. And in recent years, attackers have found ways to compromise some possession-based technologies, for example, by phishing SMS or OTP codes. Given these attacks, H-ISAC believes a better way to view authentication technology is as follows:

- Technologies that are based on a "shared secret" known by both the user trying to authenticate and the service provider asking for authentication. Passwords fall into this category, but so do other "stronger" methods of authentication, such as OTP apps and tokens as well as codes texted to users via SMS.
- Technologies that are not based on a shared secret — instead requiring that each party have just one component of what is needed to authenticate. This latter category generally relies on asymmetric, public key cryptography, as found in authentication tools using PKI or the FIDO standards.

NIST has taken a similar approach in its Digital Identity Guidelines, cautioning implementers against use of SMS codes in MFA.[3] SMS codes have proved to be vulnerable to phishing attacks, as well as SIM-swap attacks and attacks on the SS7 protocol. Likewise, token or app-based OTP solutions have also proved to be phishable, given that they are based on shared secrets. Google first flagged this issue in 2015, noting that a *"phisher can pretty successfully phish for an OTP just about as easily as they can a password."*[4] OTP codes may only be good for 30 seconds, but that is ample time for modern-day attackers to capture an OTP code and take over an account.

### Any MFA is better than no MFA

Despite these vulnerabilities, use of "shared secret" authentication tools is still better than no MFA at all, as these tools can still stop many identity-centric attacks. The goal is risk mitigation, not perfection. Wherever possible, however, H-ISAC recommends the use of high-assurance authentication, where at least one factor is based on asymmetric, public key cryptography and is thus not susceptible to phishing attacks. The good news is that high-assurance authentication is increasingly becoming cheaper and easier to use, thanks to multi-sector initiatives like the FIDO Alliance.

[3] See https://pages.nist.gov/800-63-FAQ/#q-b01
[4] See https://www.youtube.com/watch?v=UBjEfpfZ8w0

## USABILITY CAN BE AS IMPORTANT AS SECURITY

Despite the obvious security benefits, MFA adoption has lagged across healthcare and most other sectors, given the poor usability of most first-generation MFA solutions. To put it bluntly, for years the security community produced MFA tools very few people wanted to use. Technologies that require users to “break stride” to log in have alienated users. Examples of this are MFA tools that not only require a password, but then also require a user to pull out a phone or hardware token, copy a number off it, and then correctly enter it into an application. There are numerous examples of cybersecurity professionals deploying MFA, only to be told by executives to turn it off because of end-user complaints.

### Deployment Friction

When a technology solution creates a usability burden for the end user and/or adds burden to the CIO organization.

In addition, some legacy MFA tools introduced new challenges for the CIO organization, such as increased help desk calls due to user confusion, technical problems, or account recovery issues, as well as the cost of implementation and operation, and the technical difficulty of integrating a solution into existing infrastructure. These challenges increase the total cost of deploying an MFA solution.

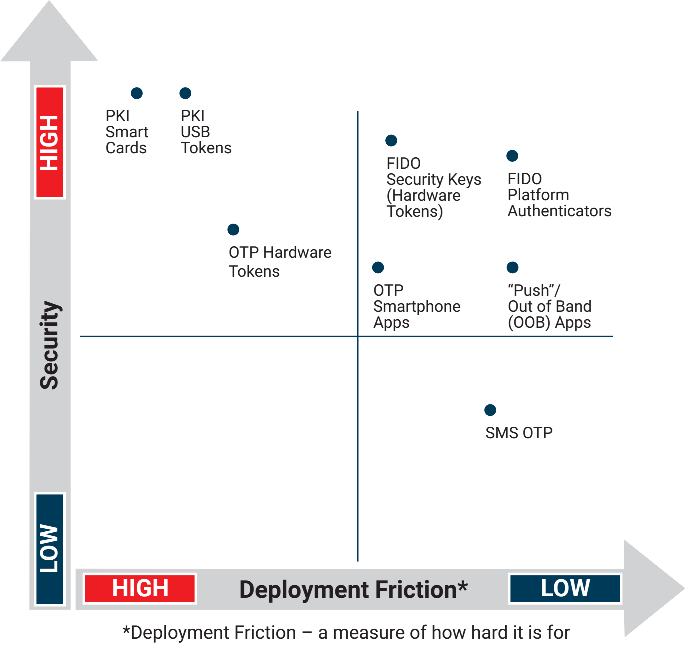
Together, these issues of usability and burden on the CIO organization create “deployment friction” that can undermine MFA implementations.

The good news is that the usability of MFA has gotten better, with next-generation MFA solutions offering streamlined authentication processes that are easier to use than passwords and cheaper for organizations to deploy and support. Google has published research on this detailing how its shift from OTP to FIDO Security Keys allowed users to log in more quickly, neutralized phishing attacks, and cut MFA-related help desk calls to nearly zero.[5]

[5] See *“Security Keys: Practical Cryptographic Second Factors for the Modern Web”* at http://fc16.ifca.ai/preproceedings/25_Lang.pdf

## A FRAMEWORK FOR HOW TO VIEW AUTHENTICATION TECHNOLOGIES

As this paper has made clear, security alone does not determine whether an MFA deployment is successful. This next section outlines a guide to different authentication technologies, viewing them from the prism of both security and deployment friction.



*Deployment Friction – a measure of how hard it is for enterprises to deploy and manage, and for people to use

## OVERVIEW OF AUTHENTICATION TECHNOLOGIES

- **Public Key Infrastructure (PKI)** hard tokens – be they smart cards or USB tokens – are the most secure for two reasons. First, because they rely on dedicated, secure hardware, and second, because there is no substitute for authentication based on asymmetric public key cryptography. The elimination of any "shared secret" component in an authentication solution means there is nothing for an attacker to phish. However, PKI has historically been complicated to implement, introducing high levels of deployment friction.

## OVERVIEW OF AUTHENTICATION TECHNOLOGIES (continued)

- **FIDO**, as the chart outlines, is a newer form of authentication that offers a balance of high security and low deployment friction. Like PKI, FIDO authentication is based on asymmetric public key cryptography, but FIDO offers "PK without the I," meaning it delivers most of the security benefits of PKI with less overhead. The user experiences are simplified. And major device, operating system, and browser manufacturers have embraced FIDO by building FIDO support into their products, making it easier to integrate and deploy.

FIDO is not delivered via a single solution or form factor. Rather, it is a capability that can be delivered through a variety of channels:

- FIDO "Security Keys" are physical hardware tokens that connect to devices over a USB, NFC, or Bluetooth interface. Security keys have proved popular in the enterprise but less so with consumers, given the need for users to carry a standalone token with them.
- FIDO "Platform Authenticators" embed the functionality of a Security Key directly in a smartphone or laptop. These authenticators leverage the fact that most modern devices ship today with protected hardware (such as the Secure Enclave in Apple devices, the Trusted Execution Environment (TEE) in Android devices, or Trusted Platform Module (TPM) chips in Windows devices) that can create, protect, and apply cryptographic keys used in FIDO authentication.

  Platform authenticators are most commonly tied to on-device matching of biometrics, allowing two factors of authentication to be delivered in a single device.

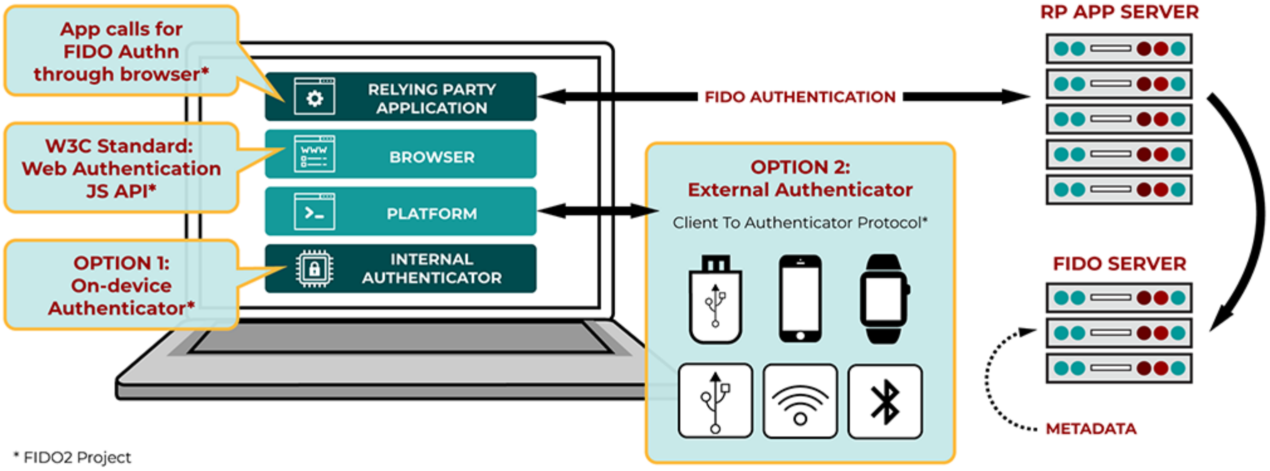
  FIDO platform authenticators can offer an improved user experience, as authentication is "built in" to devices rather than "bolted on," as is most often the case with other forms of authentication. This makes them particularly well suited for consumer-facing applications. Of note, these authenticators can be implemented in both hardware and software in the device, and security may vary depending on the implementation and device being used.

As the graphic below details, FIDO standards should be viewed as a suite of authentication tools that can be used interoperably and that include:

1. Web Authentication (WebAuthn), which is a standard web API that has been built into all major browsers and platforms to enable support for FIDO Authentication. WebAuthn is a specification developed and maintained by the W3C.[6]
2. The Client-to-Authenticator Protocol (CTAP), which defines a standardized way for use of an external authenticator — either a Security Key or a device like a smartphone that is emulating the functionality of a Security Key — to authenticate online through a device, operating system, or browser. Note that CTAP includes the legacy FIDO Universal Second Factor (U2F) standard.[7]

[6] https://www.w3.org/TR/webauthn-1/
[7] An overview of FIDO standards is at https://fidoalliance.org/specifications/

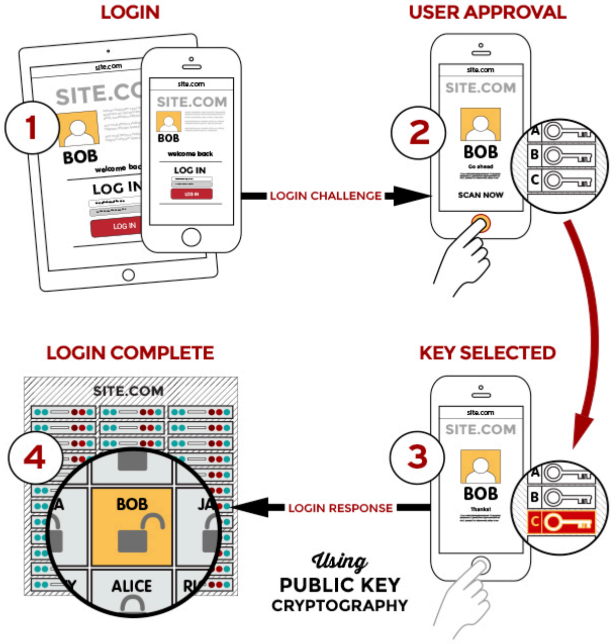
## OVERVIEW OF AUTHENTICATION TECHNOLOGIES (continued)


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
RP APP SERVER
OPTION 2: External Authenticator
Client To Authenticator Protocol*
FIDO SERVER
METADATA

* FIDO2 Project

Collectively, WebAuthn and CTAP make up the FIDO2 standards.[8]

3. FIDO Universal Authentication Framework (UAF) is an older but still widely used FIDO standard that supports a passwordless experience optimized for smartphone apps. With FIDO UAF, the users carry a device with a FIDO UAF stack installed. They can then register their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, entering a PIN, etc. The FIDO UAF protocol allows the service to select which mechanisms are presented to the user.



[8] Graphics provided by FIDO Alliance. More at https://fidoalliance.org/how-fido-works/

## OVERVIEW OF AUTHENTICATION TECHNOLOGIES (continued)

- **OTP solutions** rely on a one-time password that is generated in a standalone hardware token, or more commonly today, a smartphone app. The password changes every 30-60 seconds, which for years provided a very strong level of security against different types of credential compromises. An attacker may be able to steal a password, but without the ephemeral OTP code, the account is protected.

  As noted earlier, however, attackers have now figured out how to phish these codes through the same method that they use to phish passwords. Thirty seconds provides enough time for an attacker to execute an attack and take over an account. For guarding against attacks that are not based on phishing, OTP still provides solid security.

  A frequent complaint about OTP solutions is that they are not very user-friendly. The one thing people hate more than using passwords is having to enter their password, only to then be told to dig out their token or phone to look up and enter a second password.

- **Push notification-based authentication** offers security that is comparable to OTP — and in some cases better — while offering a better user experience. Rather than having to enter an OTP code into the computing device, users instead get a push notification on their smartphone that someone is trying to log in to their account. Touching the notification launches an authentication app, where a user is presented with a green button to confirm the authentication or a red button to reject it, as well as a notice of the online service that is the subject of the authentication request.

  Typically, push notification authentication delivers an out-of-band authentication mechanism over a mutually authenticated secure transport layer. Transaction details are displayed to the user for verification, and any discrepancies or unexpected authentication requests can be flagged with the tap of a button. Tapping the button unlocks a cryptographic key stored securely in the user's smartphone; that key is then used as the second factor to log a user in.

  One potential downside of push from a security perspective is that it may still be susceptible to phishing attacks. Just as users may be tricked into handing over their OTP code, attackers are now looking to trick people into clicking "Approve" on a push notification.

- **SMS**. The most common form of MFA is Short Message Service (SMS). In SMS, a user typically provides a mobile phone number during the creation of his or her account. Upon attempting to access the account, an OTP code will be sent to that mobile number, which will then be entered by the user.

  SMS is fairly ubiquitous and intuitive, and it makes use of technology that most individuals tend to carry with them at all times. However, SMS is among the weakest additional factors of authentication available. SMS codes are phishable and rely on the security of a user's phone. They are also vulnerable to "SIM swap" attacks, where attackers hijack a user's phone number to steal SMS codes. For these reasons, NIST in 2016 cautioned against use of SMS as an authentication factor.

  Its weaknesses aside, however, it is still better to use SMS than to use no MFA at all. SMS can still protect against many common password-focused attacks. For any application or resource where it's important to keep out a determined attacker, however, SMS is not a good choice.

# OVERVIEW OF AUTHENTICATION TECHNOLOGIES (continued)

- **Biometrics**. Ten years ago, biometrics required expensive, specialized, standalone hardware, and its deployment was largely limited to high-security facilities. Today, however, most devices ship with cameras and/or finger sensors that can be used to complement, or in some cases even replace, passwords with fingerprint or face recognition.

  Biometrics are most commonly implemented in MFA products via use of the FIDO standards, which pair an on-device biometric match with a cryptographic key to deliver single-gesture MFA. FIDO specifically limits the use of biometrics to on-device matching, mitigating the significant security and legal risks associated with systems that store or match biometrics in a centralized, networked system. And FIDO standards also provide a sort of “abstraction layer” allowing different biometric modalities and devices to be used interoperably in an organization while delivering a consistent layer of security.

  Within an enterprise, however, biometrics may also be implemented via systems that centrally store and match the biometric. This is commonly found within the health sector at provider facilities, where a patient-facing professional may be roaming from location to location and has a need to quickly log in to multiple devices. The security and privacy risks of central-match systems can be mitigated by:

  - Storing biometric templates instead of raw images
  - Placing additional security controls around this biometric information to protect it from compromise
  - Employing biometrics sensors with strong Presentation Attack Detection (PAD) capabilities to ensure that attempts to bypass biometric authentication with spoofed or counterfeit biometrics are not possible.

## You may need multiple authentication technologies

If you’ve read all this and are asking, “Do I have to pick just one?” do not fret. Depending on the type of user and the type of device they are on, different types of authenticators may be appropriate. What works well on a mobile app may differ from what works best on a browser. And what works on a laptop may not translate as well to a smartphone. By focusing on users’ “journeys” — looking at how they interact with a device or application — you can tailor authentication solutions to those journeys.

That said, it is important to make sure that you are not architecting a suite of authentication tools that has a weak underbelly. If you have implemented high-assurance MFA such as FIDO or PKI in most channels but protected one channel through SMS, an attacker can leverage that weakly protected channel to circumvent the strong authentication.

# MOVING BEYOND STATIC MFA TO CONTINUOUS AUTHENTICATION

Even use of high-assurance MFA is not enough to prevent every authentication-related attack. These days, attackers' tactics are evolving to take advantage of vulnerabilities that might allow them to take over an authenticated device or session after someone has been authenticated with MFA.

Similarly, as seen in the recent SolarWinds incident, attackers are now seeking ways to take over the Administration layer of IAM systems to issue counterfeit credentials and access tokens.

For this reason, the ultimate end goal with authentication security should not be the implementation of MFA, but rather continuous, risk-based authentication.

As described in our last paper, continuous, risk-based authentication embraces a multi-layered approach based on the following components:

- **Device authentication** can be a valuable tool for authentication and access in three scenarios:

    - If a PC, smartphone, tablet, or device has been issued by your organization
    - If the device is not issued by your organization but is managed through Mobile Device Management (MDM) or a similar capability
    - If a customer device has been used previously and can be determined to be "trusted" to an acceptable extent

    Device authentication answers a simple question: Before I think about letting a person (or service) try to access my organization's resources, are there things I know about the device they are using? Device authentication typically relies upon a certificate or browser cookie but may use other tools as well.

- **Human authentication.** Once a device is authenticated, it is important to verify that the person trying to access the resources associated with an account is the person to whom that account was issued. This is where the MFA solutions this paper previously covered are essential.

- **Analytics** are increasingly used alongside traditional authentication to continuously evaluate whether credentials are being used the way you'd expect them to be. For example, if a credential used in New York to login to a resource is then used an hour later to try to login from Moldova, that should trigger an alert that the credential may be compromised. Likewise, if someone is interacting with a known device in a way that varies greatly from their traditional patterns, that may be a sign that the device has fallen into the wrong hands.

    Effective analytics systems are able to determine if credentials are acting abnormally and can be automated to take various actions. If a credential suddenly exhibits behaviors that fall sufficiently outside the baseline of expected behavior, the system can trigger an alert, ask for additional forms of authentication, or even curb access and revoke privileges.

    At their best, analytics are integrated with both the authentication and access platform as well as the governance and administration platform. This integration can offer benefits beyond security; analytics can also streamline some authentication and access events, reducing friction for users. The Aetna case on the next page discusses such a deployment.

## MOVING BEYOND STATIC MFA TO CONTINUOUS AUTHENTICATION (continued)

- **Privileged Access Management (PAM)** focuses on applying additional controls around access to a subset of resources that are particularly sensitive. Privileged Access solutions may include session monitoring, additional layers of authentication, and other features to prevent credential compromise and limit privilege escalation.

  Privileged accounts are of particular interest to perpetrators not only because of the resources they can access, but also because other IAM controls often cannot easily detect operations performed by these accounts. Not surprisingly, many of the worst breaches of the last decade targeted privileged accounts as part of a cyber kill chain.

Together, these four layers allow organizations to deliver not just a multi-factor but also a multi-layered approach to authentication that can deliver increased security and ease the burden on end-users.

## AUTHENTICATION IN ACTION: CASE STUDIES FROM THE HEALTH ECOSYSTEM

This next section includes two case studies detailing how health care organizations are translating the ideas in this paper into practice.

As part of each case study, we asked implementers to look back at the process and the decisions that were made to note key lessons that were learned. This includes everything from “What would you do differently if you had to start over?” to “What should other companies consider if they are looking to replicate this solution?” The case studies compile these responses to provide general lessons learned and specific deployment advice.

### CASE STUDY: Aetna and Next Generation Authentication

#### Background:

Aetna (now known as CVS Health) decided several years ago to replace its legacy consumer and enterprise authentication infrastructure with a new, Next Generation Authentication (NGA) solution. Key drivers included:

- Security: Aetna’s legacy authentication solution, which relied on a purely binary (yes/no) approach, was increasingly no longer up to the task of dealing with the dynamic modern threats Aetna was encountering. The legacy solution used OTP for internal staff and Knowledge-Based Authentication (KBA) for customer-facing services; both are increasingly vulnerable.

- User experience: Adoption of a modern authentication solution provided an opportunity to improve the overall user experience by removing friction from the login process and enabling passwordless authentication. This was particularly important for users of the Aetna smartphone app.

## CASE STUDY:
## Aetna and Next Generation Authentication (continued)

### Solution:

Aetna architected a new continuous, risk-based authentication solution that combined the high-assurance capabilities of FIDO authentication with an analytics engine that delivered additional insights and capabilities into authentication events. The integration of these two tools allows Aetna to deliver passwordless logon for millions of customers.

#### *Why was this solution chosen?*

Aetna considered some interesting proprietary solutions but was worried about vendor lock-in; choosing a FIDO-based solution provided them with flexibility in that if later technical or business circumstances required a change in vendors, the transition would be made easier because of the ubiquity of FIDO standards.

On a technical level, the two core products (HYPR and Acceptto) chosen to support the FIDO and analytics portions of the NGA solution performed well and were relatively painless to integrate. They also were capable of supporting both app-based and browser-based authentication solutions.

#### *How does NGA work?*

The FIDO component delivers a high-assurance, deterministic layer of authentication based on asymmetric public key cryptography.

The analytics tool complements the FIDO element with a probabilistic layer that is able to examine signals and forecast the likelihood that an authentication event is legitimate. For many user actions, this probabilistic layer is sufficient. However, if risk signals suggest stronger authentication is needed — or if a user is attempting to engage in a higher-risk action — then the deterministic FIDO solution is triggered.

The solution is designed to work in both cloud and on-premise deployments, though for now Aetna is focused on the latter.

#### *How was it rolled out?*

Initial rollout focused on users of Aetna's mobile app; extending support to web-based users will follow. Aetna initially focused on a population of 3 million users; however, it built the infrastructure to support up to 30 million users. The solution is hosted on-premise.

A version of the solution is now being extended to internal users as well, with a focus on replacing a legacy OTP product.

The initiative is supported by a six-person project team as well as additional internal partners. The fact that it is an on-premise solution creates the need for some additional support

Aetna is building on the success of the early phases of implementation to roll NGA out to all customers and internal users. Over time, NGA may reach more than 100 million users.

# CASE STUDY:
# Aetna and Next Generation Authentication (continued)

## Results:

- No identity-related breaches of any FIDO-enabled apps.
- Call center volume tied to customer authentication problems has dropped, not only saving costs but also indicating higher customer satisfaction.
- 99.9% of users who enrolled in NGA stay in the system — nobody wants to go back to passwords.

## What lessons can other companies take away from Aetna's experiences?

1. Internal and customer-facing use cases are different. While a single core authentication infrastructure may support both, it will need to be tweaked in deployment to support each use case.
2. Having support from your organization's leadership is a must, particularly given the impact authentication has not just on security but also on user experience. Take time to explain to leaders how an NGA approach can improve both.
3. Insist on interoperability and openness in vendor solutions. Adherence to standards creates more flexibility and choices.
4. Leveraging FIDO standards allowed Aetna to give users choices in how to authenticate. One person might want to use fingerprint, a second might want face, and a third may want to use a PIN. FIDO's support for all three approaches for the user verification step of MFA enabled these choices.
5. Prioritize a great user experience and make it consistent across apps and devices. FIDO does not yet solve every problem here: Deployment in a smartphone app is different than in a browser, and the latter still has some issues around uniformity of the user experience across different browsers.
6. Keep in mind that no solution is going to be perfect and solve all your issues. Moreover, in any implementation you are going to make mistakes; arguably, you need to do so as part of working through the process to learn and get better.
7. Building extra capacity earlier also allowed the team to focus on expanding their user base without worrying about scale and capacity.

## CASE STUDY:
## Merck EngageZone

### Background:

Merck launched the Merck EngageZone solution to securely collaborate with its vendors and research partners without paying for or managing the lifecycle of their identity credentials. The solution was enabled by ensuring that all external credentials adhere to the standards and operating rules of the SAFE Identity (formerly SAFE-BioPharma) Trust Framework.[9] Key drivers included:

- Efficiency: A desire for Merck vendors to obtain credentials once and use those credentials with multiple customers for conducting clinical trials and collaboration. This would allow Merck's vendors to consolidate and reuse identities with multiple parties because the credentials are certified under the SAFE Trust Framework. Merck did not want to take on identity proofing of its vendors. Rather, Merck wanted to leverage external identity proofing by SAFE Certified Credential Providers.
- Security: The SAFE requirements mandate security standards, including robust MFA.

### Solution:

Merck built EngageZone off the Exostar Managed Access Gateway (MAG) platform.

#### *Why was this solution chosen?*

The Exostar MAG platform supported everything Merck needed to communicate with its suppliers and research partners. What separated it from other options was that the credentials provided by Exostar to Merck vendors were certified by SAFE Identity. The SAFE Trust Framework ensured that Merck vendors were not locked into a single Credential Provider; they had the option to buy credentials from other SAFE-Certified Credential Providers as well.

MAG supports both PKI- and non-PKI based (Username/Password + OTP) credentials. When using PKI credentials, Merck was able to encrypt and digitally sign sensitive communication with its partners and vendors using the same standards-based identity credentials.

#### *How does EngageZone work?*

Vendors and researchers in the Merck supply chain who needed access to a particular application within Merck were required to purchase a SAFE-certified digital identity credential commensurate with the risk associated with the application. Once the vendor obtains the appropriate credential, they used that credential to authenticate to the Merck EngageZone gateway. The Merck EngageZone is federated with Merck's business applications, which allowed Merck to use strong PKI authentication for its vendors while federating access to its business applications using SAML and SSO. This enabled sharing of ideas, discussions, documents, and other forms of communication.

The solution was designed to work in both cloud and on-premise deployments.

[9] See https://makeidentitysafe.com/ for more details.

## CASE STUDY: Merck EngageZone (continued)

### *How was it rolled out?*

The Merck EngageZone was originally designed for managing clinical trials but was later expanded to support mergers and acquisitions as well as federating with Merck's business applications.

For the initial rollout, Merck deployed in phases, focusing first on third-party partners who needed access to the EngageZone collaboration infrastructure and later focusing on federating with business applications.

### Results:

More than 65,000 people use the EngageZone solution today.

Both Merck and its partners are generally happy with the solution in that it allows all of them to enjoy the benefits of a secure, trusted identity and authentication solution, without requiring Merck to issue every credential. Stakeholders meet quarterly to provide feedback and make additional improvements.

### What lessons can other companies take away from Merck's experiences?

1. Merck notes that it would not do anything different other than enabling multi-factor authentication earlier; MFA was not part of the original deployment.

2. As a rule, if the decision is to increase security, do it as soon as possible rather than waiting because a delay will increase friction with end-users. This requires planning for the future.

3. Think about new functions the service may take on before instantiation. Case in point: Merck is using an encryption tool as part of the Merck EngageZone, which was not part of the original design.

4. Federation is increasingly supported in COTS IAM products. However, custom development may be required to federate with some custom and COTS business applications.

## CONCLUSION

Authentication is a foundational element of *An H-ISAC Framework for CISOs to Manage Identity*, and we sincerely hope that this paper has helped to clarify how different types of authentication work and to clarify misconceptions about it. By providing objective in-depth guidance on how it works, how to evaluate the differences between various solutions, and what industry best practices and standards are available, you should feel empowered to take steps to ensure your organization has implemented an appropriate solution for your use case.

## WHAT'S NEXT?

This paper represents the third release in an H-ISAC series designed to introduce CISOs to an identity-centric approach to cybersecurity. By providing an explanation of key concepts, outlining a framework and best practices, investigating the various solutions, and highlighting aspects of an effective implementation, the H-ISAC intends to provide a holistic guide to assist CISOs in the health sector on how best to approach Identity and Access Management (IAM) and its role in managing cybersecurity risk.

### *More In-depth Analysis*

Members should expect subsequent releases to provide in-depth analysis and guidance on many of the issues and technologies introduced in the first two papers.

### *Help Shape Future Papers*

As we go through this process together, your input will be vital in crafting these follow-on papers. Furthermore, we will provide a means for H-ISAC members to submit feedback as we consider future papers, so that we may ensure that this series thoroughly examines the aspects that need further clarification or elaboration. Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org.

### *Helping Organizations of All Sizes and Maturity Levels*

The H-ISAC is committed to improving the entire healthcare cybersecurity ecosystem; this series will assist organizations of any size and any cybersecurity maturity in adapting their defense models to address the current threat landscape and become more secure.

## ADDITIONAL RESOURCES

- NIST SP 800-63B “Digital Identity Guidelines: Authentication and Lifecycle Management” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
- Australian Cyber Security Centre (ACSC) Guide to MFA https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication
- FIDO Alliance https://fidoalliance.org/
- SAFE Identity https://makeidentitysafe.com/

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org

www.h-isac.org